PENTEST-SCHMERZEN

Chris Traynor

Ridgeback InfoSec, LLC

$ whoami

Chris Traynor

- Pentester at Black Hills InfoSec
- Owner of Ridgeback InfoSec, LLC
- Antisyphon Author/Instructor
  - Offensive Tooling Foundations
  - Offensive Tooling for Operators
  - BOTH now available via On-Demand**
- Certs: GSEC, GCIH, GWAPT, & GPEN

Warum ist das nötig?

- Um besser zu werden. Ganz einfach.

- Schmerzhafte Engagements haben Konsequenzen.
  - Unsicherere Umgebungen.
  - Umsatzverluste.
  - Reputationsschäden (auf beiden Seiten).
  - Rechtsstreitigkeiten.
  - Manchmal Kündigung.

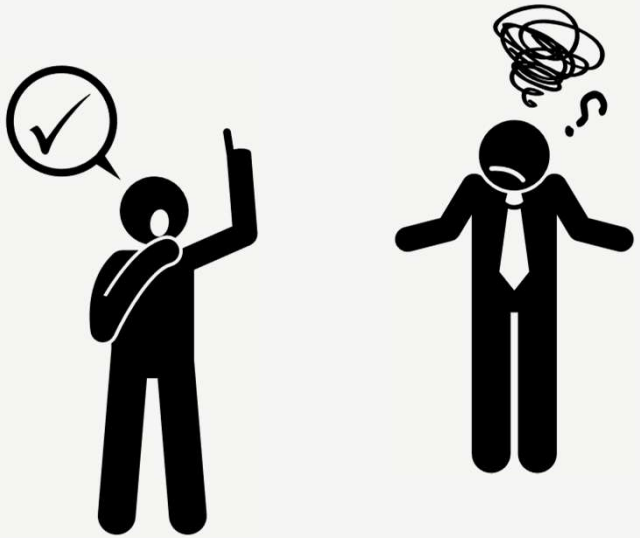
- Dies gilt für alle Beteiligten.
  - Tester, POCs, SOC-Analysten, Projektmanager usw.

- Denken Sie daran: Die meisten Engagements verlaufen gut.

Definieren Sie, was Sie tun

- Die schwierigsten Aufgaben in jedem Job sind Kommunikation und Erwartungsmanagement.
  ... nun ja... zumindest in jedem Bürojob.

- Vorurteile und Missverständnisse hinsichtlich der Ziele.
  - Pentest.
    - Web-App, Netzwerk, WLAN, physische Geräte usw.
  - Red Team
  - Purple Team
  - Social Engineering
  - Phishing



Einsatzregeln
Rules of Engagement (ROE)

- Legen Sie auf beiden Seiten POCs fest und identifizieren Sie Ersatzkandidaten.
  - Urlaub? Dienstreisen?
- Motivation für Tests
- Testtermine bestätigen
- Was fällt in den Geltungsbereich und was nicht?
- Kommunikationsrhythmus und -medium festlegen
- Notfallplan
- Genehmigung für bestimmte „risikoreiche“ Maßnahmen einholen
- Maßnahmen zuweisen
- Fälligkeitstermine vereinbaren

Vom Klienten verursachter Schmerz

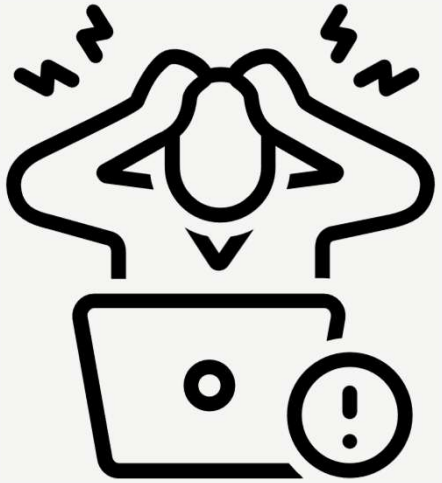
- Ungenaue oder verwirrende Scoping-Informationen
  - IPs, CIDR-Notation, FQDNs usw.
  - Duplizierte Systemlisten
  - Oftmals aufgrund von Unwissenheit über die vorhandenen Systeme.

- Nichteinhaltung von RFC 1918
  - Klasse A: 10.0.0.0 bis 10.255.255.255
  - Klasse B: 172.16.0.0 bis 172.31.255.255
  - Klasse C: 192.168.0.0 bis 192.168.255.255

- Nicht zum vereinbarten Starttermin bereit
  - Befund zur „Umweltvorsorge für Tests“

Vom Klienten verursachter Schmerz

- Feindseliges Verhalten/Spötteln
- Vorzeitige Androhung rechtlicher Schritte
- Beleidigung des Testers in persönlicher oder beruflicher Hinsicht
- Schlechte Nachrichten übel aufnehmen
- Während eines Tests nicht reagieren
- Jedes Ergebnis anfechten, um einen „sauberen Bericht“ zu erhalten
- Falsche Motivation
- Weigerung, Zugeständnisse im Interesse gründlicherer Tests zu machen
- Nicht rechtzeitig Feedback geben

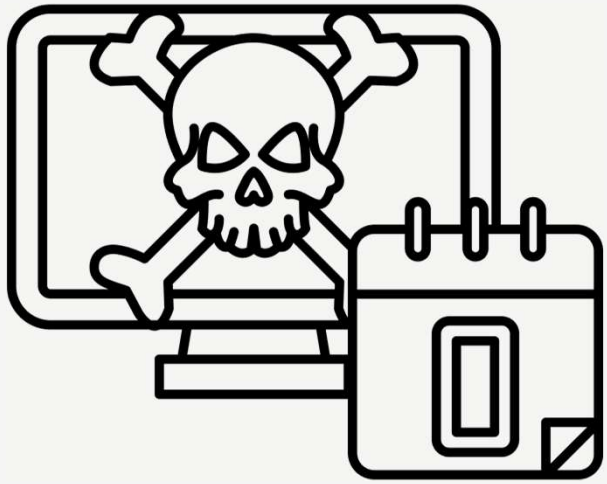


Testergesteuerter Schmerz

- Unkenntnis der eigenen Tools
  - Verwendung des falschen Tools
  - Unbewusstes Erkennen der Auswirkungen eines Tools
- Nichtüberprüfung des bereitgestellten Umfangs
- Nichteinhaltung der Liste der nicht zum Umfang gehörenden Tools
- Angriffe ohne Rücksicht auf die Branche des Kunden (Krankenhäuser, ICS usw.)
- Ausführen von DoS-Exploits
- Zu stolz, um zu fragen

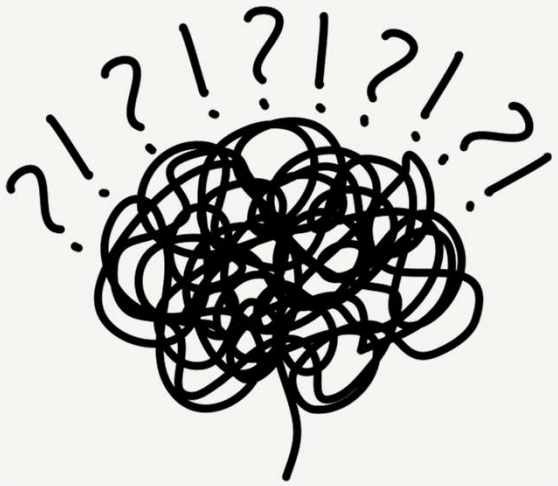
Testergesteuerter Schmerz

- Keine kontinuierliche Berichterstattung
  - Das ist ein großes Problem, Leute!**
- Ungenaue Berichte und/oder fehlende Beweise
- Der Bericht ist nicht umsetzbar
- Eine Testart übernehmen, mit der man sich nicht gut auskennt
  - Es ist in Ordnung, sich selbst herauszufordern
  - Aber lassen Sie den Kunden nicht im Stich
- Keine Kommunikation oder mangelnde Reaktion
- Liefertermine versäumen
- Unethisches oder unmoralisches Verhalten
  - Wissen, wo die Grenze liegt



Wenn etwas schief geht ...

- Beispiele:
  - Indikatoren für Kompromittierung
  - Kritische Ergebnisse
  - Fehler in Berichten
- Denken Sie daran: Wir sind alle im selben Team.
- Lassen Sie sich nicht von Ihrem Ego beeinflussen.
- Kommunizieren Sie schnell und professionell.
- Dokumentieren, dokumentieren und dokumentieren Sie.
- Wissen, wann eskaliert werden muss.
- Sie müssen nicht der Böse sein.



THANK YOU

FOR ATTENDING

Chris Traynor

blackhillsinfosec.com

antisyphontraining.com

ridgebackinfosec.com